IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

COHEN SEGLIAS PALLAS GREENHALL & FURMAN, P.C. **Plaintiff**	:	CIVIL ACTION
v.	:	NO.
DEFENSE INFORMATION SYSTEMS AGENCY; **UNITED STATES ARMY CYBER COMMAND;** **JOINT FORCES HEADQUARTERS;** **and** **UNITED STATES DEPARTMENT OF THE ARMY** **Defendants.**	:	

COMPLAINT

Plaintiff, Cohen Seglias Pallas Greenhall & Furman, P.C. ("Plaintiff" or "Cohen Seglias"), by and through its undersigned counsel, brings this action against the Defense Information Systems Agency ("DISA"); the United States Army Cyber Command ("ARCYBER"); Joint Forces Headquarters ("JFHQ"); and the United States Department of the Army acting through the U.S. Army Corps of Engineers, Middle East District, ("USACE"), (collectively, "Defendants"), and alleges as follows:

JURISDICTION AND VENUE

1. This Court has jurisdiction over this matter pursuant to 28 U.S.C. § 1331 as this action arises under the laws of the United States, including, but not limited to, the Administrative Procedure Act, 5 U.S.C. §§ 701-706. Venue is proper in this District pursuant to 28 U.S.C. § 1391(e) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

PARTIES

2. Plaintiff is a law firm with its principal place of business in Philadelphia, Pennsylvania, with offices in Washington, DC, and other cities. Plaintiff includes a legal practice group that focuses on federal government contract law and regularly conducts business with various federal agencies, boards of contract appeals, and federal courts.

3. Defendant, Defense Information Systems Agency ("DISA") is part of the United States Department of Defense ("DoD"), and plays a crucial role in ensuring the secure and reliable communication and information sharing capabilities essential to U.S. military operations. DISA is tasked with a variety of functions aimed at supporting the defense and military communities, including the management of IT and communication systems that are vital to the U.S. military's command and control functions. This includes everything from email systems to secure messaging and voice communication networks.

4. Defendant, United States Army Cyber Command ("ARCYBER") focuses on protecting and defending U.S. Army networks and ensuring the operational readiness of its forces in the digital domain. This includes implementing robust security measures, monitoring network activity to detect and respond to threats, and ensuring compliance with cybersecurity policies and standards.

5. Defendant, Joint Forces Headquarters ("JFHQ") refers to a component of the U.S. military's command structure designed to oversee and coordinate the activities of specific military operations, often within a particular domain such as cyberspace, or a geographic region. Their mission includes focusing on cyber operations, such as the Joint Force Headquarters-Cyber (JFHQ-Cyber), their function includes overseeing cyber defense operations, coordinating

offensive and defensive cyber activities, and ensuring the protection of critical information networks.

6. Defendant United States Department of the Army ("USACE"), acting through the U.S. Army Corps of Engineers, Middle East District, is an agency of the United States Government.

7. Defendants, collectively, are agencies believed to be responsible for the actions complained of herein.

FACTUAL ALLEGATIONS

8. On or about March 22, 2024, Plaintiff discovered that it was not receiving email messages from any U.S. Department of Defense ("DoD") mail servers originating from the email domain ".mil" including, for example, army.mil, navy.mil, af.mil, mail.mil. It should be noted that email messages from the Armed Services Board of Contract Appeals ("ASBCA") use the "mail.mil" domain name and the Plaintiff has many Contract Disputes Act appeals, on behalf of its clients, pending before the ASBCA.

9. Plaintiff subsequently learned that Defendants had, without warning or any valid reason, placed an Email Reputation Service ("ERS") block on the cohenseglias.com domain "due to an ongoing risk on the site that was detected as recently as March 19, 2024." As further explained below, the alleged "risk" was not specifically identified, other than a vague reference to the possibility that malware was being hosted. This "block" prevented federal agencies under Defendants' control from sending email messages to Plaintiff's attorneys.

10. An ERS block means that the domain "cohenseglias.com" has been placed into IP address database that intercepts outgoing email messages and prevents their transmission. Unfortunately, in this case, the block was imposed by mistake and it was only after noticing that

anticipated responses from government agencies were not being received that the Plaintiff discovered that there was a block.

11. This ERS block was imposed without notice to Plaintiff, and federal agencies were unaware of the block because their outgoing email messages did not generate bounce-back messages. Plaintiff was similarly unaware that communications were being sent and not received. Curiously, email messages sent by the Plaintiff to federal agencies were received by those agencies. In other words, the block was one-sided and only affected outgoing email messages from the federal entities

12. Plaintiff's Government Contracting Group was formed in 2009 and has represented hundreds of government contractors in matters involving federal agencies and has never, until now, suffered an interruption of email service. The law firm receives thousands of emails daily, including many from federal agencies that do not have a ".mil" email address without encountering any problems.

13. In fact, in the approximately 15 years before this unwarranted ERS block was imposed, the Plaintiff has not encountered a single interruption or blockage of its email service from any source, and most assuredly not from any federal government site.

14. Upon discovering the ERS block, Plaintiff promptly contacted Army IT personnel at USACE, who were very cooperative and explained that Defendant DISA would need to address the issue.

15. Out of an abundance of caution, Plaintiff's IT personnel contact the firm's own email security gateway service, Mimecast, to determine whether the Plaintiff's security protocols were blocking the incoming messages. Mimecast reported that no email messages from ".mil"

had been blocked by the Plaintiff's system and, in fact, there was no indication that any message from ".mil" had been received by the Plaintiff's email server.

16. Plaintiff then contacted its Web hosting service that controls its email service, to determine whether they could identify any reason for the blockage at the Plaintiff's end. The Web hosting service performed a scan and reported that there was nothing on the Plaintiff's system that was preventing the receipt of email messages from ".mil" and that there was nothing of a suspicious nature that could have served as a red flag to any federal agencies. This was later reported to DISA.

17. On advice from USACE, on or about March 28, 2024, Plaintiff's IT personnel contacted the Global Service Desk at Defendant DISA to seek their assistance and were informed that USACE needed to submit a ticket, known as an infrastructure request, before DISA could investigate the matter. USACE reported, later that day after submitting the ticket, that DISA had declined to take remedial action because Plaintiff's email server and website had been found to contain malware. However, the prior security scan by Plaintiff's Web hosting service had confirmed that this was not the case.

18. On March 29, 2024, Plaintiff's IT personnel contacted DISA again and asked what else could be done. DISA instructed Plaintiff to contact the Joint Forces Headquarters ("JFHQ") who was responsible to coordinate such matters with various DoD agencies. JFHQ informed Plaintiff that it could only remove the ERS block if another agency, ARCYBER, agreed to "accept the risk" and authorized JFHQ to take remedial action.

19. Subsequently, on April 3, 2024, JFHQ advised Plaintiff to Contact ARCYBER and they instructed Plaintiff to submit all of its background information on the problem to a group mailbox.

20. ARCYBER replied to Plaintiff's IT personnel on April 5, 2024 and stated that a request for assistance would need to come from USACE and could not come from the Plaintiff (even though ARCYBER had asked Plaintiff to send it all of the background information). Furthermore, ARCYBER stated that USACE would need to submit a ticket request to DISA in order to get the process started. This process, it was explained, would require USACE and DISA to investigate the cause of the block.

21. Plaintiff, on April 5, 2024, informed ARCYBER that a ticket had already been submitted by USACE to DISA on March 29, 2024 bearing Ticket No. 2990466. ARCYBER stated that they had not received any of the required test results which should have been obtained by USACE and DISA.

22. The prior history notwithstanding, DISA required USACE to submit a new ticket on April 5, 2024 and Ticket No. 2993696 was promptly furnished.

23. What followed was a classic example of Plaintiff being handed off from one Defendant to another with no resolution in sight as Plaintiff attempted to obtain a status update. The only information that was reported by ARCYBER, orally, was that Plaintiff's servers had been identified as "vulnerable" for unspecified reasons.

24. On information and belief, the Defendants USACE and DISA have not performed the testing that is required to validate the security of Plaintiff's Website and email hosting server, and nothing is being done to authorize JFHQ to unblock Plaintiff's receipt of email.

25. Plaintiff's website and email server do not host malware or any inappropriate content and any such violation would have been quickly detected and removed by the firm's own security gateway, Mimecast, if it actually existed.

26. The ERS block imposed by the Defendants was caused by a malfunction or computer "glitch" on their end and they have failed to grasp the urgency of this matter and the need to take appropriate and swift remedial action.

27. It is inconceivable that something occurred overnight on March 22, 2024, that overcame 15 uneventful years of electronic communication by Plaintiff without incident. Significantly it is only the ".mil" email extension that is being blocked and no other Website, federal agency, board of contract appeals (other than the ASBCA), or federal court has failed to communicate with the Plaintiff.

28. Despite Plaintiff's diligent efforts to resolve the matter, and after over two weeks of waiting with no remedy in sight, Defendants have failed to lift the unwarranted block, necessitating this action.

29. On April 12, 2024, a further status inquiry to DISA was made and the reply was "If there is no further risk detected the block would be removed on/around 18May." This is outrageous and the Plaintiff should not be required to wait that long for the Government to correct its mistake.

30. The Plaintiff is caught in a bureaucratic quagmire with no federal agency willing to promptly address the issue for which the Defendants are solely responsible.

31. The lack of any sense of urgency, or sincere interest in a prompt remedy, by the Defendants is outrageous and warrants immediate relief.

COUNT I: VIOLATION OF THE ADMINISTRATIVE PROCEDURE ACT

32. All preceding paragraphs are incorporated herein by reference.

33. Defendants' actions in blocking Plaintiff's ERS and failing to remedy the situation upon notification are arbitrary, capricious, an abuse of discretion, or otherwise not in accordance

with law, and lack observance of procedure required by law, in violation of the Administrative Procedure Act, 5 U.S.C. §§ 706(2)(A) and (D).

COUNT II: REQUEST FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY AND PERMANENT INJUNCTIVE RELIEF

34. Plaintiff hereby incorporates by reference all preceding paragraphs.

35. Plaintiff has a substantial likelihood of prevailing on the merits of its request. The Defendants' imposition of an ERS block on Plaintiff's domain without valid justification, proper notice, or procedure violates applicable law, including the Administrative Procedure Act.

36. Plaintiff has no adequate remedy at law to redress the injuries it is suffering. The nature of the block prevents timely and essential communications with federal entities, impacting Plaintiff's legal practice and its ability to serve its clients effectively. Monetary damages cannot compensate for the loss of time-sensitive opportunities and the potential adverse impact on Plaintiff's professional reputation.

37. Plaintiff is suffering and will continue to suffer irreparable harm if the ERS block is not immediately removed. The block impedes critical communications required for adherence to legal deadlines and for the conduct of ongoing legal matters, thereby threatening Plaintiff's legal practice and the interests of its clients.

38. The balance of hardships tips decidedly in favor of Plaintiff. Removing the ERS block would not impose a significant burden on Defendants, whereas maintaining the block inflicts substantial harm on Plaintiff and its clients.

39. Granting the requested injunctive relief would serve the public interest by ensuring the uninterrupted flow of communication between legal counsel and federal entities, which is essential for the proper administration of justice.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

A. Declare that Defendants' actions in imposing and maintaining the ERS block on Plaintiff's domain without valid reason or proper procedure are unlawful;

B. Issue a Temporary Restraining Order directing Defendants to immediately remove the ERS block on "cohenseglias.com," pending a full hearing on a preliminary injunction, based on the following:

i. Plaintiff's substantial likelihood of prevailing on the merits;

ii. The lack of an adequate remedy at law;

iii. The irreparable harm being suffered by Plaintiff;

iv. The balance of hardships tipping decidedly in favor of Plaintiff; and

v. The service of the public interest.

C. Schedule a prompt hearing on Plaintiff's motion for a preliminary injunction;

D. Award Plaintiff its costs and reasonable attorney's fees incurred in bringing this action; and

E. Grant such other and further relief as the Court deems just and proper.

Respectfully submitted,

COHEN SEGLIAS PALLAS GREENHALL & FURMAN, PC

BY: *_/s/ Michael H. Payne_*

Date: April 18, 2024

Michael H. Payne, Esquire (Bar No. 09846)
1600 Market Street, 32nd Floor
Philadelphia, Pennsylvania 19103
Tel.: (215) 564-1700
mhp@cohenseglias.com
Attorney for Plaintiff